

**In the claims:**

1. A method for providing highly secure access of a partner to the development environment of another partner comprising the steps of:  
starting a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password;  
starting a session by the partner in a Web page on a portal machine that authenticates through LDAP the user/password of the person;  
routing the session to an engagement box depending on the person where the engagement boxes are on network segments separated by firewall boxes with another logon/password and is validated thru second LDAP and wherein all users of the same partner are all launching on the same box ; and  
accessing data and applications from that engagement box on Network File system storage authenticated LDAP to get benefit of a big compute farm composed of many high-end servers in a very secure way.
2. The method of Claim 1 including the step of submitting batch or interactive jobs to a server farm on a common resource segment so data input and data output on the server farm remains on a common resource but the remote display is going back to the engagement box of the partner.
3. A method of enabling a collaborative network with partners without compromising Intellectual Property comprising the steps of:

providing a highly secure common resource computing zone with services such as design and production wherein data input and output remains on the secure common resource computing zone; and

providing layers of security to separate engagement boxes for each of the partners in said secure common resource computing zone where the partners can work simultaneously, run simulation tests, emulate software problems and share in said secure common resource computing zone with just the remote display going back to the engagement box of the partner and therefore to the partner outside the owner.

4. The method of Claim 3 including the step of said partners running local applications on said engagement boxes such as design applications, mail, editor, etc. or on a server farm segment that resides on the secure common resource computing zone for bigger batch or interactive jobs.
5. The method of Claim 3 including the step of providing a backend segment that includes an intranet access through a firewall to an owner's intranet.
6. The method of Claim 5 including the step of providing an access box for management of all critical boxes in said secure computing zone.
7. The method of Claim 3 wherein said providing layers of security step includes the steps of:  
  
starting a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password;

starting a session by the partner in a Web page on a portal machine that authenticates through LDAP the user/password of the person; routing the session to an engagement box depending on the person where the engagement boxes are on network segments separated by firewall boxes with another logon/password and is validated thru second LDAP and wherein all users of the same partner are all launching on the same box ; and accessing data and applications from that engagement box on Network File system storage authenticated LDAP to get benefit of a big compute farm composed of many high-end servers in a very secure way.

8. A system for providing highly secure access of a partner to the development environment of another partner comprising:

means for providing a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password;

means for starting a session by the partner in a Web page on a portal machine that authenticates thru LDAP the user/password of the person;

means for routing the session to an engagement box depending on the person where the engagement boxes are on network segments separated by firewall boxes with another logon/password and is validated thru second LDAP and wherein all users of the same partner are all launching on the same box ; and

means for accessing data and applications from that engagement box on Network File system storage authenticated LDAP to get benefit of a big compute farm composed of many high-end servers in a very secure way.

9. The system of Claim 8 including means for submitting batch or interactive jobs to a server farm on a common resource segment so data input and data output on the server farm remains on a common resource but the remote display is going back to the engagement box.
10. A system for enabling collaboration by an owner of a collaborative network with partners such as sub-contractors, customers and/or Electronic Design Automation (EDA) vendors without compromising Intellectual Property comprising:  
a highly secure common resource computing zone with services wherein data input and output remains on the secure common resource computing zone; and  
means for providing security to separate engagement boxes for each partner in said secure common resource computing zone where the partners can work simultaneously, run simulation tests, emulate software problems or share in said secure common resource computing zone with just the remote display is going back to the engagement box of the partner and therefore to the partner outside the owner.
11. The system of Claim 10 wherein said partners can run local applications on said engagement boxes such as design applications, mail, editor, etc or on a server farm segment that resides on the common resources zone for bigger batch or interactive jobs.
12. The system of Claim 10 including a backend segment that includes an owner's intranet access through a firewall to an owner's intranet.
13. The system of Claim 12 including an access box for management of all critical boxes in said secure computing zone.
14. The system of Claim 10 wherein said means for providing security includes

means for providing a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password;

means for starting a session by the partner in a Web page on a portal machine that authenticates thru LDAP the user/password of the person;

means for routing the session to an engagement box depending on the person where the engagement boxes are on network segments separated by firewall boxes with another logon/password and is validated thru second LDAP and wherein all users of the same partner are all launching on the same box ; and

means for accessing data and applications from that engagement box on Network File system storage authenticated LDAP to get benefit of a big compute farm composed of many high-end servers in a very secure way.